U.S. Customs and Border Protection

Passenger Systems Program Directorate

Automated Passport Control Service Release 2.0 Interface Control Document

January 30, 2017

Document Number: 3209000-ICD, v11b

Change Control Log

Revised by	Date	Description of Revisions
(b)(6); (b)(7)(C)	08/01/2012	Initial Document.
	08/27/2012	Updated to include most recent comments and changes.
	08/29/2012	Updated to include most recent comments and changes.
	10/04/2012	Updated to add networking information.
	10/23/2012	Updated Sequence Diagram and APC references.
	10/25/2012	Updated diagrams and document formats.
	11/05/2012	Technical review and editorial updates.
	11/13/2012	XML and editorial updates.
	11/29/2012	Reconcile this document with APC WSDL and schema definitions.
	12/06/2012	Updated tables and diagrams.
	12/17/2012	Updated diagrams, phrasing, content placement and flow.
	12/21/2012	Updated tables and diagrams as a result of schema changes.
	12/27/2012	Updated message references and diagrams
	01/28/2013	Updated section language and added in Fault Message Table
	01/29/2013	Updated contact details, section 2.1.1 Kiosk System order and Environment Information table
	01/29/2013	Updated column headers in the Environment Information table
	04/22/2013	Updated Environment Information (IP Addresses)
	05/09/2013	Updated the schema diagram and tables to match the current schema resulting from release 1.2.(b) (7)(E) (b) (7)(E)
	06/07/2013	Updated Referral Code descriptions and hierarchy
	06/10/2013	Updated Section 4.1.2.2 Environment Information
	06/14/2013	Added SAT information to Section 4.1.2.2
	07/15/2013	Updated for APC 2.0
	07/15/2013	Updated Section 3.1.1, Table 7, and Section 3.3
	07/25/2013	Added more clarity to several element descriptions in Section 3. Updated transaction time specification table in Section 4.
	07/25/2013	Add examples for fingerprint software names and versions elements
	10/28/2013	Add sample Traveler Request XML message to section 3.1.1.1.3
	11/19/2013	Schema, table, and XML sample updates

Revised by	Date	Description of Revisions
(b)(6); (b)(7)(C)	11/21/2013	Review and overall document refinements
	11/22/2013	Review and overall document refinements
	11/22/2013	Diagram updates, final review and overall document refinements
	11/25/2013	Incorporated client revisions and other document refinements.
	02/19/2014	Incorporate revisions for SOAP messages and Vessel Processing
	04/21/2014	Overall document reorganization
	04/22/2014	Incorporate revisions for LPR
	06/16/2014	Incorporate clarification that a fault terminates session
	06/24/2014	Incorporate clarification of four finger slap
	08/11/2014	Incorporate Kiosk assignment of SF and CA Referral Codes
	10/09/2014	Clarified characteristics of fingerprint image
	01/14/2015	Incorporated Visa Processing (Document Type VN/VB) and support for Canadian LPR Biometric data collection.
	01/28/2015	Formatted and edited to PSPD standards
	02/17/2015	Incorporated review comments
	03/11/2015	Incorporated Enhanced Declarations
	03/12/2015	Removed the Capability Indicator
	05/08/2015	Incorporated Security recommendations, updated document and contact information.
	12/22/2015	Clarified criteria for a single session ID for all members of a family group
	04/25/3016	Remove FlightList and Manual ADD; set DailySecurityCode to optional; Document Reorganization
APC Team	07/25/2016	Defined Declarations as Optional to accommodate sites for which collection of declaration information would be a violation of Customs laws.
APC Team	09/01/16	Clarified Fingerprint Image
APC Team	10/11//16	Clarified Referral on failure to confirm flight, Photo guidelines and rules related to printed referral prior to session initiation.
APC Team	11/21/16	Clarified acceptance of Five Declaration question responses.
APC Team	12/12/16	Specified Naming Convention for Seaport Kiosks
APC Team	01/20/17	Clarified Requirement for System Status

Table of Contents

Table of Figures and Tables

Automated Passport Control Service / Kiosk System Interface Control Document

1. Introduction

1.1 Purpose

The purpose of this document is to provide the interface specifications between the Kiosk System and the U.S. Customs and Border Protection (CBP) Automated Passport Control (APC) Service. This document provides a high-level overview of the technical architecture, describes the message request and response dialogues, outlines message components, and provides data validation rules. For purposes of this document the term "Kiosk" includes authorized entry devices which may be devices physically installed at ports or mobile devices using an approved application. The term "Kiosk System" is used to refer to the third-party system interfacing with the APC Service.

1.2 System Overview

APC is a service for ports wanting to utilize third-party self-service kiosks and other entry devices to support CBP primary processing of international travelers. The APC Service will perform initial traveler vetting and manifest lookups for the third-party kiosk system. The APC Service is designed to support the following types of travelers entering the US at international Airports and Seaports:

- United States Citizens presenting a US Passport.
- Canadian Citizens presenting a Canadian passport and entering under B1 or B2 Class of Admission.
- Citizens of Visa Waiver Countries presenting a Passport from their Country of citizenship, entering under WB and WT Class of Admission, who are enrolled in the Electronic System for Travel Authorization (ESTA).
- United States Lawful Permanent Residents (US LPR) presenting a C1 or C2 document.
- Travelers presenting a United States Nonimmigrant Visa Document (Document Types VN or VB) for entry under Class of Admission B1, B2 or D1 (Visa Class Codes B1, B2, B1/B2, D1, and C1/D).

The APC Service is an internet-facing web service that the Kiosk System will utilize to allow a traveler or traveler group to complete an expedited inspection.

1.3 Background

CBP is one of the Department of Homeland Security's largest components. CBP is responsible for protecting the United States' front line, while facilitating legitimate trade and travel. CBP is continuously working to improve the entry process for the traveler and realize the goal of increased security while expediting the flow of legitimate travel. The goal of the self-service kiosk in a CBP environment is to allow a traveler or family unit to complete a portion of an inspection prior to speaking with a CBP Officer.

The intent of the kiosk system is to collect traveler information and transfer that information to CBP for law enforcement and border inspection purposes. A self-service kiosk option has been added to the Airport Technical Design Standard (ATDS), allowing Port Authorities the option to use kiosks to facilitate data collection. CBP/OIT worked to develop a technology requirements package to provide to interested port authorities. Under the ATDS, Port Authorities can opt to incorporate kiosks as equipment in their respective Federal Inspection Services (FIS) areas. Stationary kiosk equipment and supporting servers are provided by, maintained, and owned by the Port Authority. Any kiosk procured and installed by a Port Authority must comply with DHS/CBP security requirements, Automated Passport Control Services technology requirements and meet CBP Business requirements. Similarly, any kiosk application operating on a mobile device must comply with DHS/CBP security requirements, Automated Passport Control Services technology requirements and meet CBP Business requirements.

1.4 Contact Information

Questions and comments related to this ICD should be sent to the APC OIT Group (b) (7)(E) Please note: Questions and comments related to Business requirements and Kiosk design should be addressed to the Office of Field Operations (b) (7)(E)

1.5 Document References

The documents were used as references for this APC Service / Kiosk System ICD.

Table 1. Document References

User Reference Document Name	Document Identification Number	Location
2012-2016 Border Patrol Strategic Plan	2012-2016 Border Patrol Strategic Plan	(b) (7)(E)
DHS Sensitive Systems Policy Directive 4300A Version 11.0, April 30, 2014	DHS National Security Systems Policy Directive 4300A	(b) (7)(E)
National Institute of Standards and Technology Special Publication 800-64, Revision 2, Security Considerations in the Information System Development Life Cycle, October 2008	NIST 800-64 Rev. 1	(b) (7)(E)

The following APC documentation is relevant to this ICD:

- Automated Passport Control Service / Kiosk System Onboarding Guide
- Business Requirements (BRD)
- Technical Reference Manual (TRM)
- Interface Control Document (ICD), including the Environmental Supplement and APC Service's WSDL and XML schemas
- Automated Passport Control Integration Test Plan
- APC Frequently Asked Questions (FAQ)

2. System Description

2.1 System Architecture

Figure 1 illustrates the recommended high-level system components and interfaces used in the APC Service. The principle components are the Kiosk System and the APC Service. The Kiosk System requests information from the APC Service while the APC Service interacts with various CBP systems to obtain a response relevant to the Kiosk System's request.

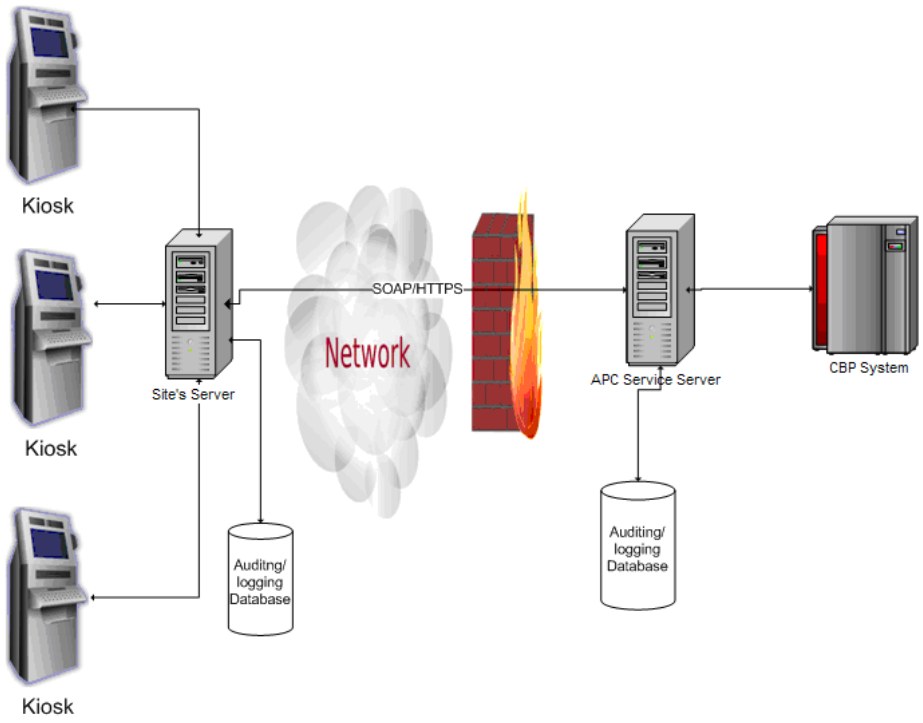


Figure 1. APC Service High-Level Technical Architecture

Each port will utilize a single SSL Certificate to communicate with the CBP production site. A separate SSL certificate will be required for communication between the port non-production environment and CBP's non-production (test) environment. The one non-production certificate will be used for communication with both the CBP System Acceptance Test (SAT) and the CBP Quality Assurance (QAX) environments.

2.2 Kiosk System

The Kiosk System is a self-service entry point used by Port Authorities to collect traveler information and transfer that information to CBP for law enforcement purposes. The Kiosk System is: (1) a piece of equipment in the form of a kiosk or other CBP approved device that allows a traveler to input data, and (2) a server(s) that allows the kiosk to interface with CBP's APC Service for traveler processing. The Kiosk System is neither managed nor implemented by CBP; third-party vendors are responsible for its system implementation. While it interfaces with the APC Service to request traveler processing data, the Kiosk System is isolated from CBP's

internal networks and systems.

The following functions are performed by the Kiosk System:

- Meet the business, technical, and operational requirements
- Display information and instructions to the traveler(s)
- Collect the necessary travel information from each traveler
- Collect biometrics from traveler(s) when relevant
- Prepare and send the Traveler Validate Request(s)
- Process vetting results from the Traveler Validate Response message
- Request and receive the Traveler End message
- Prepare and print or display receipts for traveler as specified
- Record and document session information
- Request and receive the APC Service system status message
- Process APC generated Fault messages

2.3 APC Service

The APC Service is a web service that implements the high-level requirements described in this section. The APC Service is the primary interface to CBP for the Kiosk System. The APC Service and the Kiosk System support the overall goal of the Automated Passport Control program.

The following functions are performed by the APC Service:

- Read and validate the Traveler Validate Request(s)
- Calculate the referral code according to the business rules for each traveler
- Prepare and send the Traveler Validate Response message
- Read and validate the Traveler End Request from the Kiosk System
- Prepare and send Traveler End Response(s)
- Prepare and send the Border Crossing record notifications to the appropriate CBP subsystems
- Read and validate the System Status Request
- Prepare and send System Status Response
- Prepare and send Fault response when required

The APC Service is hosted in the CBP National Data Center (NDC) and supported by the CBP Office of Information Technology (OIT) network and operations center. This center monitors and supports the network and servers to provide connectivity and system monitoring between the port and NDC.

2.4 APC Web Service Dialogues

The APC Service provides four web service dialogues that allow the Kiosk System to request information from the APC Service. In each of the four dialogues, the Kiosk System initiates the message request and the APC Service provides a message response. The web services operations are:

- Traveler Validate
- Traveler End
- System Status

The System Status request allows the client to obtain the current state of the APC Service. Upon receiving the request, the APC Service sends a response indicating whether or not APC is available for processing.

Traveler Validate and Traveler End dialogues are used in sequence as part of an interactive workflow that processes a traveler. The **TravelerValidateRequest** is sent from the kiosk to initiate vetting processing of a traveler for a border crossing; the APC service returns a **TravelerValidateResponse** with the initial vetting results. The kiosk, in turn, sends a **TravelerEndRequest** to the APC Service notifying the service to complete traveler processing. Upon completion of processing the APC service returns a **TravelerEndResponse** to the kiosk which serves as authorization for the kiosk to print the traveler receipt. For integrity of operations, with the exception of a System Failure (SF) or Cancel (CA) referral code, the APC Service interface requires that the kiosk receive a valid **TravelerEndResponse** message from APC Services prior to printing/displaying the traveler receipt. The Kiosk may print a System Failure (SF code) receipt in events where faults are received from the APC Service or in events where the vendor provided APC system fails to transmit the final dialog message to the APC Service. The Kiosk system presents a Cancel (CA) referral code when a traveler session is cancelled for reasons other than failure to confirm the presented flight information. When the traveler declines to confirm the presented flight information, the kiosk vendor should print the Referral code specified in the Business Requirements statement. The kiosk vendor is referred to OFO and the Business Requirements statement for handing traveler cancellation prior to submission of any information to the APC service.

Figure 2 illustrates the message dialogue between the Kiosk System and the APC Service.

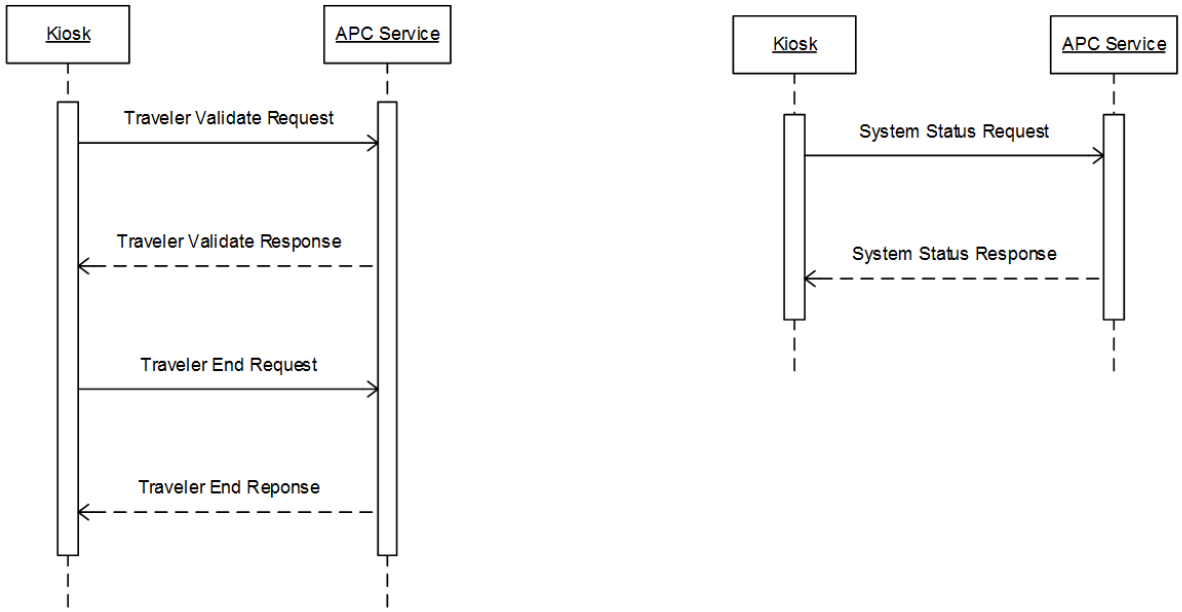


Figure 2. APC Service Message Dialogue

2.5 Key Processing Fields

Processing fields critical to the APC Service include the Kiosk Identifier, the Session Identifier and the Traveler Identifier. The length of these three fields should comply with the following guidelines:

A. **The length of the three fields KioskID, SessionID and TravelerID shall not exceed 47 characters.**
B. The KioskID, assigned by the APC OIT Group, is a fixed length of 10 Characters
C. **The SessionID shall not exceed 20 characters in length and the sum of the SessionID length plus the TravelerID length shall not exceed 37 characters.** It is recommend that the SessionID include a time stamp to milliseconds resolution plus any additional values required to ensure the KioskID plus SessionID is unique. **The same SessionID must be assigned to all members of a family group;** the Session ID must not include Personally Identifiable Information (PII).
D. **The TravelerID shall not exceed 20 characters in length and the sum of the SessionID length plus the TravelerID length shall not exceed 37 characters.** The combination of the KioskID plus SessionID plus TravelerID shall be unique. The TravelerID must not include PII.

The following conventions are defined for these fields:

- **Kiosk Identifier** – The KioskID must be unique system wide. The KisokID identifies the traveler's physical position to the port and terminal within the port (when there is more than one international terminal). CBP will assign KioskIDs upon receipt of a request from the Port Authority. There

  The standard kiosk format for Airport Kiosks is pppmcctnnn where

  - ppp is the Port Code

- m is the mode of transportation (A=Air, S=Sea)
- cc is a constant (currently "PC" for Kiosks, "MC" for Mobile)
- t is the terminal identifier
- nnn is the unique kiosk number within the port and terminal. (e.g. AIR: AUSAPC1001, YYZAPC3010)

The standard kiosk format for Seaport Kiosks is pppmccttnn where

- ppp is the Port Code
- m is the mode of transportation (A=Air, S=Sea)
- cc is a constant (currently "PC" for Kiosks, "MC" for Mobile)
- tt is a two character terminal identifier
- nn is the unique kiosk number within the port and terminal. (e.g. SEA: FLLSPC1801)

The KioskID shall adhere to the ISO/IEC 8859-1 character set [A-Z][0-9].

Internally, the APC/MPC system maintains a relationship between the Port/Terminal identification embedded within the KioskIDand a site ID. This must be a one-to-one relationship such that all Kiosks associated with a single SiteID have the same Port/Terminal assignment and, conversely, all kiosks with a common Port/Terminal Identifier be associated with a single SiteID. In some instances this may mean the original request for a Port/Terminal Identifier cannot be honored

- **Session Identifier** – The Kiosk Identifier plus Session Identifier, generated by the kiosk/kiosk application, must be distinct and unique **system wide**. The SessionID must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9]. CBP suggests the following approach:

  yyyyMMDDHHmmssSSSxx, where yyyyMMDDHHmmssSSS is the date/time group to milliseconds and xx is a suffix to ensure uniqueness of the Session Identifier.

  The xx suffix may not be required for stationary kiosks. Non-stationary kiosks which serve multiple concurrent sessions may need to incorporate the suffix to ensure uniqueness of the session identifier. The SessionID must be the same for all members of a family group; the SessionID must not include PII.

- **Traveler Identifier –** The TravelerID, assigned by the Kiosk/kiosk application, must be distinct and unique within a session. The TravelerID must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9]. The combination of SessionID + KioskID + TravelerID must be unique. The TravelerID must not include PII.

The following standards apply to the port codes, Carrier Codes, Flight numbers, and Country Codes and Names.

- **Airport and Seaport Codes** are based on the three character IATA definitions.
- **Carrier codes and flight numbers** are based on International Civil Aviation Organization (ICAO) definitions and will be based on what the carriers transmit in the

manifests. This information is sent to the CBP's Advance Passenger Information System (APIS). The Vessel Code is based on the International Maritime Organization (IMO) Ship Identification Number (IMO Number).

- **Country Codes and Country Names** are based on the ISO 3166-1 3-character standard.

2.6 APC Service Message Domain Models

The APC Domain Model, Part 1 is presented in Figure 3; Part 2 is presented in Figure 4Figure 4.

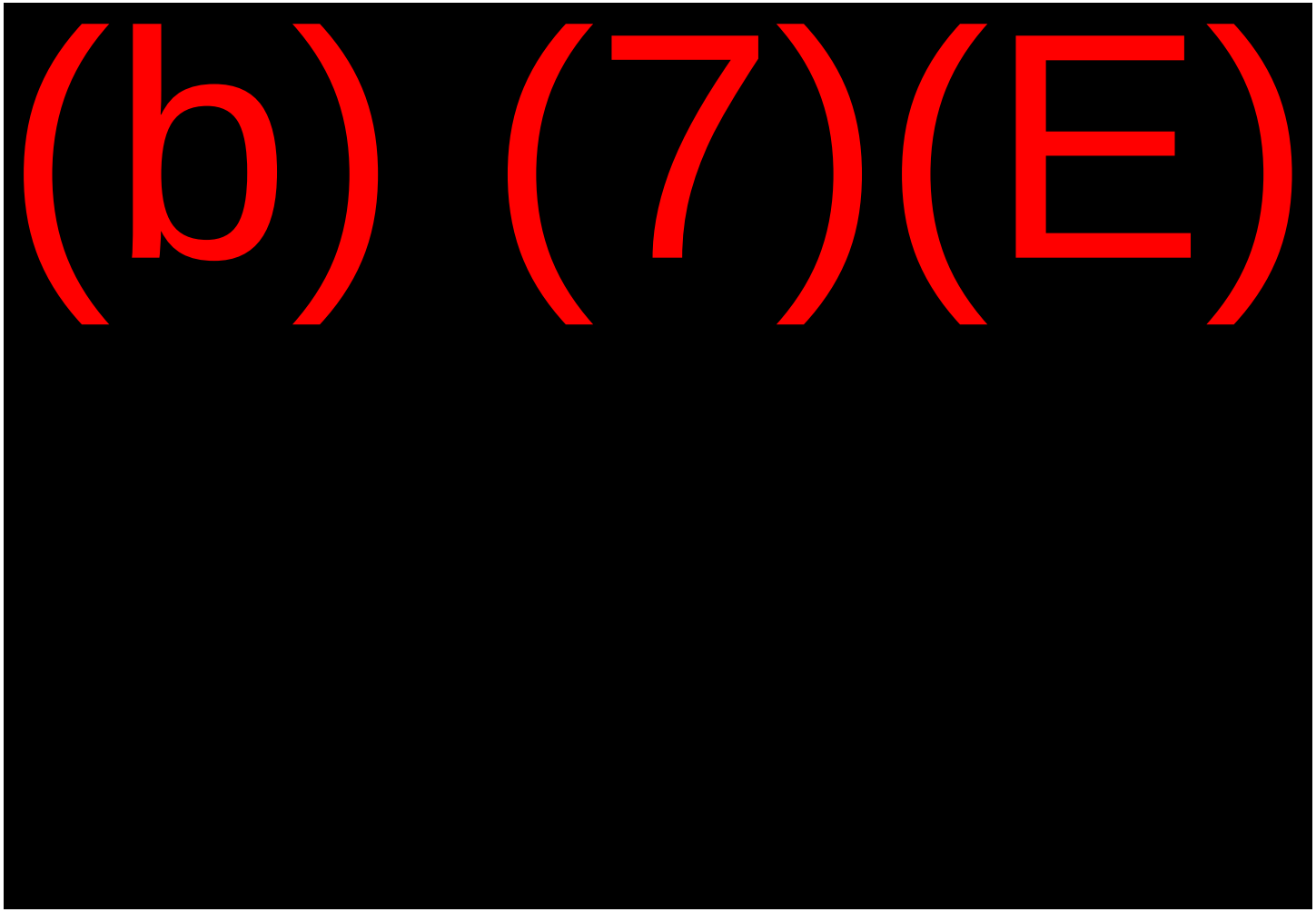


Figure 3. APC Service Message Domain Model, Part I

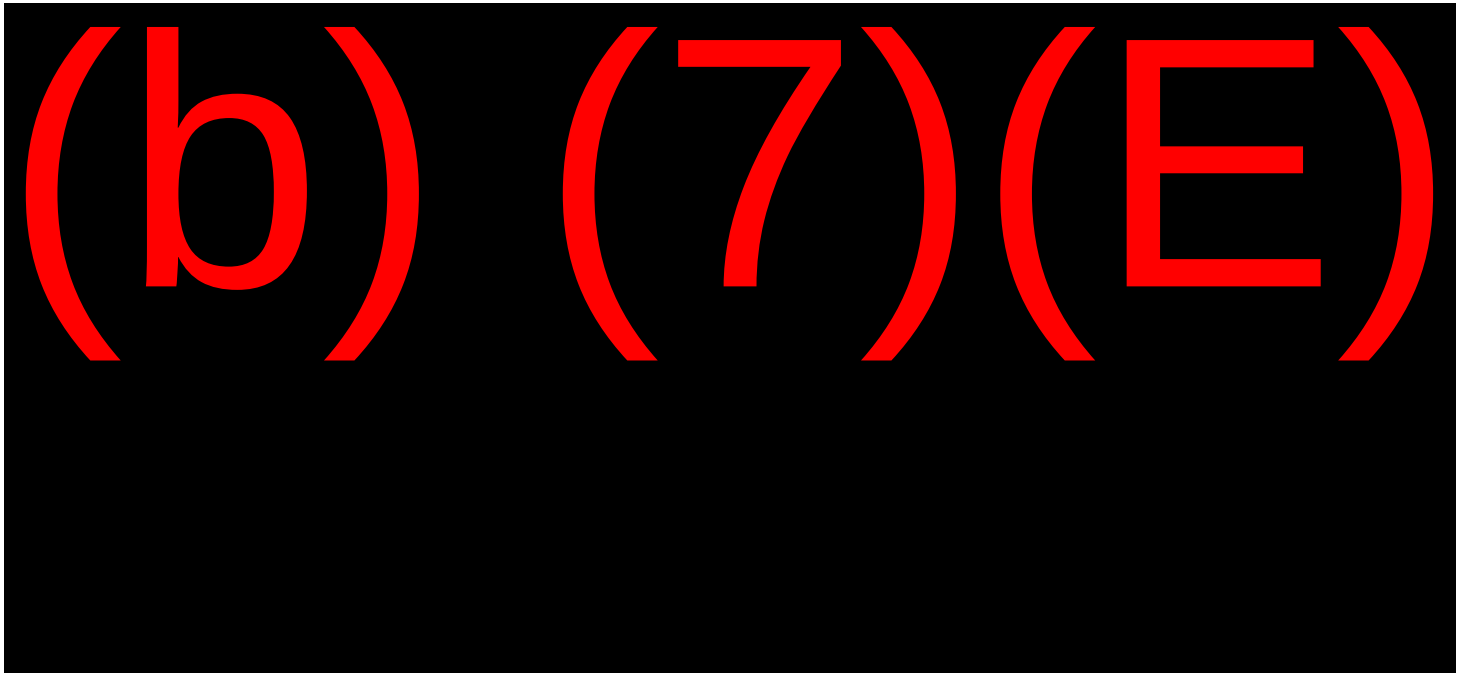


Figure 4. APC Service Message Domain Model, Part II

3. Photo and Fingerprint Specifications

3.1 Photo Capture Specification

Photographic images should be ICAO conformant, meaning the face image would be captured as a digital photograph using JPEG, JPEG 2000, PNG, etc. The utility of a face image for either machine or human recognition is highly dependent on the quality of the photograph; therefore APC refers to the ICAO standards as "best practices" assuring a high quality capture. It is recommended that any Data Entry Point (DEP) mechanism ensures a face photograph maximizes as many ICAO quality parameters as possible, in order to translate into better identification services. The key parameters relate to size of the face relative to the full image frame, the angle, pitch, and yaw of the subject's head, and the evenness and intensity of the lighting. To the extent that subjects are cooperative and habituated to the DEP, simple mechanisms for adjusting lighting, focus, and size (e.g. zoom) and then snapping the picture when the subject's head is at the right angle all increase quality.

A recommended approach is to employ a "quality in the loop" image capture step that employs software capable of analyzing the image and then controlling the shutter. There are several commercial and non-commercial software packages that can be used to add this quality loop. The preferred parameters are:

- Pose: Full Frontal or Frontal Token
- Angle: +/- 5 degrees in all three dimensions
- Expression: Neutral
- Eyes: Open with >90 pixels from pupil to pupil
- Background: plain with no texture
- Lighting: No shadows or point lighting
- Size: Minimum 640 x 480 pixel
- Face Size: >1/2 width of frame and >3/4 height of frame
- Camera: 24 bit color
- Images shall possess true symmetry and not be reversed mirror images

Appendix A documents specifications and best practices for facial image capture.

3.2 Fingerprint Captured Biometrics

This section defines fingerprint image criteria and image quality thresholds applicable to Fingerprint Captured Biometrics sent to the APC Service for processing.

3.2.1 Fingerprint Image

One fingerprint image shall be provided. The image shall comprise the four fingers of either hand, thumb excluded. Fingerprints shall have a class resolution at least 19.69 ppmm (500 ppi) and shall be processed in.wsq (Wavelet Scalar Quantization) format. The image must not exceed 500 KB. The image dimension must be no more than 1500H x 1600W. The variable-resolution fingerprint image data contained in the record may be in a compressed form.

A list of FBI-approved forensic grade products can be found at the following link: http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_cert. Selection of the FBI

Certified Products List shows commercial products that have passed the FBI's technical specifications and are acceptable for capture and transmission of biometrics to the APC Service for processing.

3.2.2 NFIQ Scores

A National Institute of Standards and Technology (NIST) Fingerprint Image Quality (NFIQ) number is a prediction of a matcher's performance; it reflects the predictive positive or negative contribution of an individual sample to the overall performance of a fingerprint matching system.

NFIQ has five levels of quality thresholds that are intended to be predictive of the relative performance of a minutia based fingerprint matching system, where an NFIQ score of 1 is the highest quality, and an NFIQ score of 5 is the lowest. Refer to Table 2. NFIQ Scores for required NFIQ scores for each associated finger.

Table 2. NFIQ Scores

Number of Finger	Name of Finger	NFIQ Required Scoring
1	Right Thumb	1-2
2	Right Index	1-2
3	Right Middle	1-2
4	Right Ring	1-2-3
5	Right Pinky	1-2-3
6	Left Thumb	1-2
7	Left Index	1-2
8	Left Middle	1-2
9	Left Ring	1-2-3
10	Left Pinky	1-2-3

A list of certified software vendors that meet FBI standards for Wavelet Scalar Quantization (WSQ) Gray-scale Fingerprint Image Compression Algorithm exchanges can be found at the following link: https://www.fbibiospecs.org/wsq/Implementations/Default.aspx.

4. Message Exchange Specifications

4.1 WSDL and XML Schemas

The APC WSDL provides definitive guidelines for message exchange between the kiosk application and the APC Service. The APC Service's WSDL is available for use in application development. In the event of a discrepancy between the WSDL and this ICD, the WSDL takes precedence.

All character data submitted must adhere to the ISO/IEC 8859-1 (Part 1, Latin-1 Western European) character set; restrictions are specified where applicable. Separate specifications are given within the body of this document for image data.

The APC Service transactions are a simple request/response data exchange via SOAP web services. There is a 1:1 ratio between a request and a response and errors are managed via SOAP web services fault handling. NIEM is used to implement the XML data structures for the APC Service.

Subsequent sections of this ICD define the elements of message calls between the Kiosk System and the APC Service and specify APC processing criteria and constraints. Kiosk developers should leverage Web Service tools from JAX-WS, WCF or the platform of their choice to generate source that will create and validate messages for the APC Services. Other interactive tools that can validate messages against the schema like SoapUI can be useful for testing the interface during development.

It is expected that the Kiosk System will perform XML validation on an XML message to confirm that the message is well-formed and valid before sending the data to the APC Service.

The URLs for accessing the APC WSDL and XML schemas are documented in the Environmental Supplement to this ICD. This supplement is available to approved vendors upon request to the APC OIT Grou (b) (7)(E)

The WSDL includes Flight List Request and Response elements that are not documented in this ICD version. Current Business Requirements obviate the need for Flight List services. Flight list elements have been retained in the WSDL to support existing service pending implementation of the new Business Requirements relevant to Flight Confirmation.

4.2 National Information Exchange Model (NIEM)

The National Information Exchange Model (NIEM) is used to implement the XML data structures for the APC Service. The use of NIEM is DHS mandated and it provides the basic data types for XML validation.

Information on NIEM can be found at http://www.niem.gov/.

4.3 Message Exchange

Message Exchange between the Kiosk System and the APC Service consists of requests and responses to invoke the APC Service functions.

Specifications for Request messages are presented in Section 4.4 of this document; specifications for Response messages are presented in Section 4.5. The Sample messages that are provided in

these subsections are presented as examples only.

Each message element is defined in terms of the following characteristics:

- **Element** – The name of the element.
- **Data Type** – The type of data that defines the element.
- **Size** – The maximum size of the data type. An asterisk "*" denotes there is no limit on the size (i.e., unbounded). A format of "x | y" indicates the minimum and maximum size of an element that has a collection of values. A "--" indicates that the size is not applicable; see the element's data type instead. In general, when a size is specified for a String type it is considered the maximum useful length. String fields that are longer than the specified data format may be truncated.
- **Rqd** – Whether or not the element is required; "Y" for yes and "N" for no. Note, a required element does not mean that the element value is not nullable. Refer to the APC Service xml schemas for specific detail.
- **Description** – The purpose of the element.

Data types that are commonly referenced in the schema elements are described in Table 3.

Table 3. Common Data Type Definitions

Data Type	Format or Allowed Values	Description

Boolean	Allowed Values:
	`true`
	`false`
		A binary indicator denoting either true or false. Values conform to the NIEM `niem-xsd:boolean` format.

CountryAlpha3Code	Allowed Values: *See ISO 3166 alpha-3 country codes.*	The three letter identification of a country as defined by ISO 3166 alpha-3.
Date	Format: `YYYY-MM-DD`	A date value that conforms to the NIEM `niem-xsd:date` format.
DateTime	Format: `YYYY-MM-DDThh:mm:ssTZD`	A date and time value that conforms to the NIEM `niem-xsd:dateTime` format.

SexCode	Allowed Values:
	`F`
	`M`
	`U`
		A code value that identifies the gender of a person. "F" indicates female, "M" indicates male and "U" indicates unknown/unidentified.

Data Type	Format or Allowed Values	Description
String	n/a	A value consisting of a series of alphanumeric characters that is encoded in UTF-8 format. Strings can be of unlimited length unless where noted. The type conforms to the NIEM **`niem-xsd:string`** format with the following modifications: • Lowercase alphabetical data will be converted to uppercase letters in the response message. • Spaces will remain as spaces. • Non-alphabetical and non-numeric characters will be converted to spaces when used for searching.

4.4 Request Messages

Each of the following request messages may be sent by the Kiosk:

- Traveler Validate Request
- Traveler End Request
- System Status Request

The corresponding response element specification can be found in Section 4.5

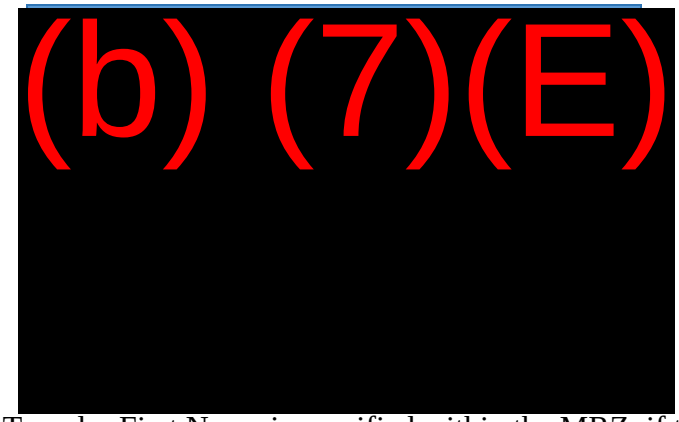
4.4.1 Traveler Validate Request

The request for validation of the traveler data is initiated by the Kiosk System using the **TravelerValidateRequest** message element. The elements that comprise the message request are displayed in Table 4 through Table 13. The APC service uses the SessionID to tie together all members of a family group. As documented in Table 13, the same SessionID must be assigned to all members of a family group. Each member within the group is uniquely identified by the assigned TravelerID.

For all traveler submissions which are based on read of the Machine Readable Zone (MRZ) of the traveler document, the kiosk should apply basic integrity verification to the MRZ Read. Specifically, the kiosk should not forward to APC any Traveler Validate Request for which the MRZ read does not meet the following criteria:

- The MRZ length is 88 characters for Passports Document type VN; the MRZ length is 90 characters for Document Types VB, C1, and C2.
- The document expiration date in the MRZ is not earlier than the date the document is submitted to APC.
- Each character of the Traveler first and last names is an alphabetic character (Special Characters and Numeric Characters are not allowed).
- The Date of Birth extracted from the MRZ is a valid date.
- For US Issued Visas, the VISA Class code embedded in the MRZ is consistent with a Class of Admission accepted by APC; only MRZ class codes valued (B1, B2, B3, B5, C4 or D1should be transmitted to APC. The Class of Admission specified by the traveler

must be consistent with the Class code encoded in the MRZ. The following table applies:



- The Traveler First Name is specified within the MRZ; if the MRZ does not include a first name, the traveler should not be submitted to the APC system.
- The Traveler Citizenship code must be present in the MRZ.

For any MRZ read which fails this basic criteria, the kiosk should not initiate an APC session for the traveler and should refer the traveler in accordance with OFO guidelines and the Business Requirements.

Additionally, when fingerprints are collected, the kiosk should ensure the following:

- The quality score for each fingerprint should be between 1 and 4.
- Four prints are submitted.
- The angle of the hand should be between 65 and 115 degrees.

Prints which do not adhere to the above criteria should not be submitted. Either new prints should be collected or the kiosk should cancel the session with no transmission to APC.

Multiple members of a family may be processed under a single session identifier; each member is assigned a unique Traveler ID. The kiosk should also ensure that the same traveler document is not submitted more than once within a session.

Figure 5 shows an example of the **TravelerValidateRequest** SOAP message.

Table 4. TravelerValidateRequest Element

TravelerValidateRequest				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
KioskID	String	10	Y	A system wide unique identifier for the kiosk. Must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9]; special characters are not allowed. Assigned by the APC OIT Group
SessionID	String		Y	A value that uniquely identifies the session. Must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9]; special characters are not allowed. The SessionID plus TravelerID should not exceed 37 characters. The SessionID

TravelerValidateRequest				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
				must be the same for all members of a family group; travelers not in a group are assigned their own Session ID. The combination of KioskID plus Session ID must be unique for an individual or for all members of a family group.
TravelerID	String		Y	The unique identification value associated with the traveler for the session. Must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9]; special characters are not allowed. The SessionID plus TravelerID should not exceed 37 characters. The KioskID plus SessionID plus TravelerID must uniquely identify a traveler. For a family group, the SessionID identifies all members of the group and the TravelerID identifies each member uniquely.
ManualEntryInd	Boolean		Y	If set to false then the traveler document data was scanned and the MRZ is required. If set to true then the traveler document data was entered manually and the following elements are used to identify the traveler: PersonGivenName, DocumentExpirationDate, PersonSurName, PersonBirthDate, PersonSexCode, PersonCitizenshipCode, DocumentNumber, DocumentIssueCountryCode, and DocumentType. Data must be entered exactly as it appears in the MRZ. Manual entry is only accepted for US and Canadian Passport Travelers (document type=P) from services for which OFO has authorized use of Manual Entry.
MRZ	String	100	C	Data read from the MRZ. Required when ManualEntryInd=False
ManualEntry	ManualEntryType		C	Manual Entry of PassengerData. Required when ManualEntryInd=true
DeclarationQuestion	DeclarationQuestionType	--	C	Element comprising the declaration questions/responses that are asked of the traveler. Occurs five times, one for each declaration question. Element with both

TravelerValidateRequest				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
				attributes populated is mandatory for sites permitting collection of Declarations; this element must not be included for sites that do not allow collection of Declarations.
FingerprintCapture	FingerprintCaptureType	--	C	The biometric capture of the traveler. Reference the Business Requirements for the categories of travelers for which biometric data must be submitted. The APC service will return a fault if biometric data is not submitted for a traveler who requires biometric vetting.
ClassOfAdmissionCode	ClassOfAdmissionCodeType	-	C	The code that indicates that type of travel being conducted by the traveler in the country. Required for all foreign nationals including Canadians. Not Applicable to US citizens and US LPRs. Visa Waiver must specify WT or WB. Canadians must specify B1 or B2. Visa Travelers must specify B1, B2, or D1.

The Manual Entry Element is only applicable when ManualEntryInd = “true” in the **TravelerValidateRequest** Element. Data Submitted in the Manual Entry Element must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9] $!;#% and space. Fields must be entered as they appear in the MRZ. Currently use of the manual entry element is authorized for mobile devices only and should only be used by mobile devises when the traveler does not scan the document. When the traveler submits a scanned document to the mobile application, the mobile application should set ManualEntryInd = “false” and should supply the scanned information in accordance with the above specifications. Kiosk vendors must secure OFO and OIT approval for use of this element.

Table 5. Manual Entry Element

ManualEntry				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
PersonGivenName	String	50	Y	The first name and middle names of the traveler exactly as they appear in the MRZ of the travel document
DocumentExpirationDate	Date	--	Y	The expiration date of the document provided by the traveler exactly as it appears in the MRZ of the travel document.
PersonSurName	String	50	Y	The last name (surname) of the traveler exactly as it appears in the MRZ of the travel document.
PersonBirthDate	Date	--	Y	The birth date of the traveler.
PersonSexCode	SexCode	--	Y	The gender of the traveler.
PersonCitizenshipCode	CountryAlpha3Code	3	Y	The code of the country where the traveler has citizenship.
DocumentNumber	String	16	Y	The number assigned to the document from the document's issuing office exactly as it appears in the MRZ of the travel document.
DocumentIssueCountryCode	CountryAlpha3Code	--	Y	The code of the country that issued the document of the traveler.
DocumentType	String	2	Y	The type of document. Must be valued P.

The DeclarationQuestion element is presented in Table 6. Inclusion of this element is conditional on whether collection of Declarations information is allowed by Customs laws at the site where APC is operational. Each APC Site will be designated as DeclarationsMandatory or DeclarationsExempt.

The majority of APC sites are designated DeclarationsMandatory. For DeclarationsMandatory sites, one occurrence of the DeclarationQuestionElement must be included for each required declaration question. For the current APC implementation, a maximum of four occurrences of the DeclarationQuestion Element can be submitted. For sites authorized to accept Declarations, the APC Service will accept five declaration responses; the APC service will also accept four Declaration responses to support existing kiosks until all kiosks are upgraded to five responses. For sites that are authorized to ask Declarations, each of the component attributes (DeclarationQuestionNumber and DeclarationQuestionSelectedIndicator) must be populated. If the required DeclarationQuestionElement is not included in the request from a DeclarationsMandatory site, the APC Service will return a fault.

The DeclarationQuestionElement should not be included in the TravelerValidateRequest for any site designated DeclarationsExempt. The APC service will return a fault response if

TravelerValidateRequest is received from a DeclarationsExempt site with a DeclarationQuestionSelectedIndicator attribute included.

Table 6. DeclarationQuestion Element (Applicable to Sites Designated DeclarationsMandatory)

DeclarationQuestion				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
DeclarationQuestionNumber	DeclarationQuestionNumberType	--	Y	A code that identifies the declaration question. Mandatory for sites except those designated Declarations Exempt. Declarations Exempt sites are directed to omit the declarations Element entirely and not populate any attribute within the element.
DeclarationQuestionSelectedIndicator	Boolean	--	Y	The true or false value that was provided by the traveler in response to the associated question. Mandatory for sites except those designated Declarations Exempt. Declarations Exempt sites are directed to omit the declarations Element entirely and not populate any attribute within the element.

The FingerprintCapture element is required for all travelers between the ages of 14 and 79 (<80) except for US and Canadian Passport Travelers. The APC Service will return a fault response to the kiosk if a **TravelerValidateRequest** is received for a traveler who requires Biometric Data submission but for whom the data is not submitted. (Reference the Business Requirements for details on the travelers for whom biometric data must be submitted.). The APC will also return a fault response when the transmitted fingerprints do not adhere to the specification for fingerprint submission. The kiosk should not submit a traveler who requires fingerprints if a valid set of fingerprints cannot be supplied. Fingerprint submissions require valid entries for Fingerprint Position codes and for Print Quality.

Travelers requiring biometric verification must be preregistered in the IDENT system. The APC Schema provides for a four-finger slap, thumb excluded. The kiosk should not submit the FingerprintCaptureElement for any traveler who does not require Biometric data collection.

Table 7. FingerprintCapture Element

FingerprintCapture				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
TravelerPhotoImage	PhotoImageCaptureType	*	Y	A base 64 ICAO conformant face photo image of the traveler. The image must not exceed 192KB; jpeg is recommended.
FingerprintImage	PhotoImageCaptureType	*	Y	Capture of the traveler's four-finger slap. The four finger slaps shall have a class

FingerprintCapture				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
				resolution at least 19.69 ppmm (500 ppi) and shall be processed in.wsq (Wavelet Scalar Quantization) format. The image dimension shall be no more than 1500H x 1600W and the size shall not exceed 500 KB.
IsImageConcatenated	Boolean	--	Y	A true value indicates that the fingerprint image is concatenated and false indicates that it is not.
IsCapturePlatenDirty	Boolean	--	Y	A true value indicates that the fingerprint platen is dirty and false indicates that it is not.
CaptureDeviceMakeText	String	25	Y	The manufacturer of the fingerprint scanner. e.g. - "Cross Match"
CaptureDeviceModelText	String	25	Y	The model of the fingerprint scanner. e.g. - "GuardianV900251RevA"
CaptureDeviceSerialNumberText	String	50	Y	The serial number of the fingerprint scanner. e.g. – "000550782.B2007"
CaptureDeviceFirmwareVersionText	String	50	Y	The firmware version of the fingerprint scanner. e.g. – "V95.35 LSCAN 500C (c) CMT"
ClientApplicationSoftware	SoftwareDetailType	--	Y	The name and version of the client application software. e.g. – "APC" (software vendor name) "2.0" (software vendor version)
ImageQualitySoftware	SoftwareDetailType	--	Y	The name and version of the fingerprint quality scoring software used during the capture. e.g. – "Cogent" (software vendor name) "10.7.2" (software vendor version)
ImageFeatureExtractionSoftware	SoftwareDetailType	--	N	The name and version of the fingerprint image feature extraction software used during the capture. It is recommended this attribute be populated with no value. This element will be removed in a future release of the schema.
Fingerprint	Software	--	Y	The name and version of the fingerprint

FingerprintCapture				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
CompressionSoftware	DetailType			image compression software used during the capture. e.g. – “Aware NFIQ” (software vendor name) “10.9.8” (software vendor version)
IndividualFingerDetail	FingerprintSegmentType	--	Y	The coordinates of the fingerprint segments in the slap image.

Table 8. PhotoImageCapture Element

PhotoImageCapture				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
Image	Base64	--	Y	The image that was captured; a base 64 encoded photo.
ImageHeight	Integer	--	Y	The height of the image in pixels.
ImageWidth	Integer	--	Y	The width of the image in pixels.
CaptureDate	DateTime	--	Y	The capture date of the image.
CaptureTime	DateTime	--	Y	The capture time of the image.
CaptureDuration	Duration	--	Y	The capture duration of the image. The duration should be the period of time that the fingerprint screen is being displayed.

Table 9. SoftwareDetail Element

SoftwareDetail				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
SoftwareVendorNameText	String	50	Y	The name of the software vendor.
SoftwareVersionNumber	String	50	Y	The version number of the software.

Table 10. FingerprintSegment Element

FingerprintSegment				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
FingerPositionCode	Integer	--	Y	A code that identifies the finger position. The acceptable codes are:

FingerprintSegment				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
				2 – Right index finger 3 – Right middle finger 4 – Right ring finger 5 – Right little finger 7 – Left index finger 8 – Left index finger 9 – Left ring finger 10 – Left little finger
IsMissingOrUnavailable	Boolean	--	Y	A value of true if the finger was unable to be captured or missing and false if the finger is available in the capture.
FingerprintSegmentDetail	FingerprintSegmentDetailType	--	N	Provides detailed segment data of the finger identified in FingerPositionCode. When IsMissingOrUnavailable value is false then this element is required. When IsMissingOrUnavailable value is true this element is ignored.

Table 11. FingerprintSegmentDetail Element

FingerprintSegmentDetail				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
XCoordinate	Integer	--	Y	The top left x-coordinate position of finger in the slap image.
YCoordinate	Integer	--	Y	The top left y-coordinate position of finger in the slap image.
Height	Integer	--	Y	The height, in pixels, of the finger in the slap image.
Width	Integer	--	Y	The width, in pixels, of the finger in the slap image.
QualityScore	Integer	--	Y	The NFIQ quality score for the finger.
VendorScore	Integer	--	Y	The vendor quality score for the finger.

Table 12. DeclarationQuestionNumber Enumeration Element

DeclarationQuestionNumber Value	Description
ONE	The declaration question posed to the traveler that is identified as

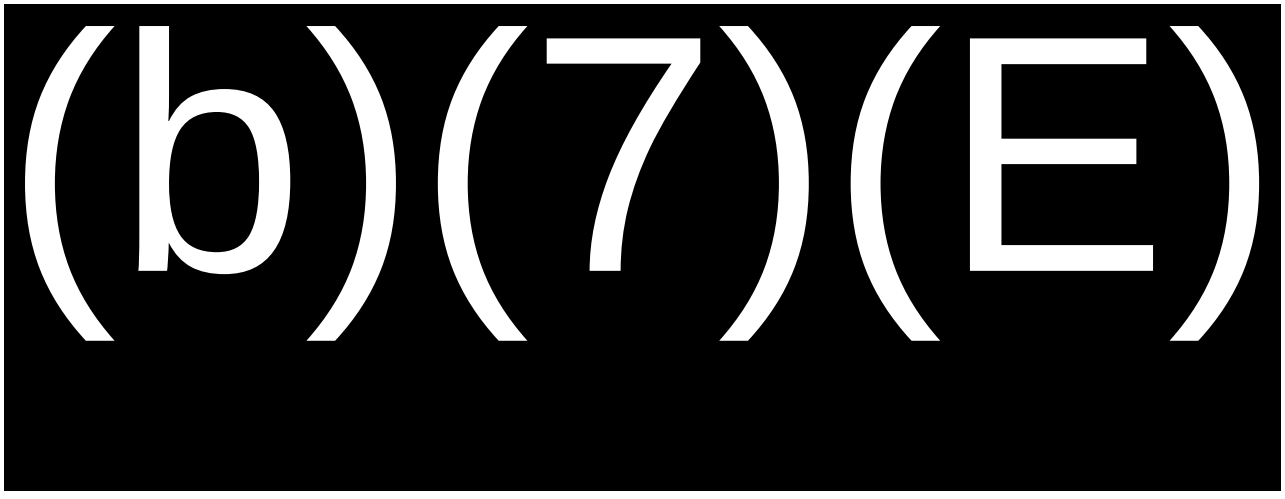
DeclarationQuestionNumber Value	Description
	question "1."
TWO	The declaration question posed to the traveler that is identified as question "2."
THREE	The declaration question posed to the traveler that is identified as question "3."
FOUR	The declaration question posed to the traveler that is identified as question "4."
FIVE	The declaration question posed to the traveler that is identified as question "5." (Note: this value is not authorized in the current APC Schema. This information is provided to support vendor design efforts. OFO will notify vendors when the value is authorized.)

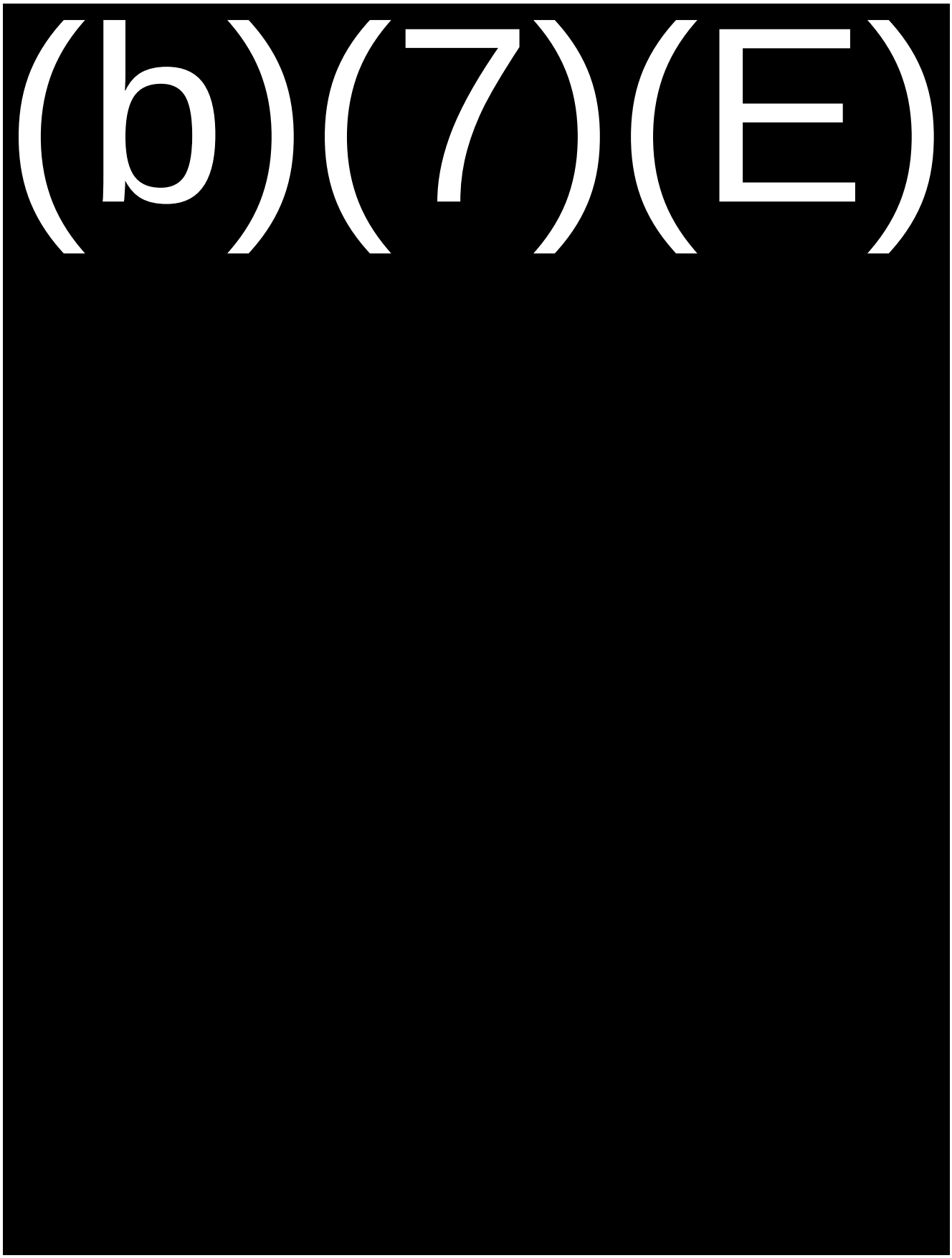
To allow for expansion as required, the ClassOfAdmissionCode is not an enumeration element. The following table identifies the values that APC currently accepts depending on the Document Type being processed.

Table 13. ClassOfAdmissionCode Values Accepted (Not an Enumeration Element)

ClassOfAdmissionCode	
Value	**Description**
B1	Nonimmigrant Temporary visitor for business (including Peace Corps).
B2	Nonimmigrant Temporary visitor for pleasure.
D1	Nonimmigrant Temporary visitor Crew.
WB	For business purposes under the Visa Waiver Program
WT	For pleasure purposes under the Visa Waiver Program

Note the following example of a TravelerValidateRequest is for a site requiring collection of Declaration information (non-exempt site).




(b)(7)(E)

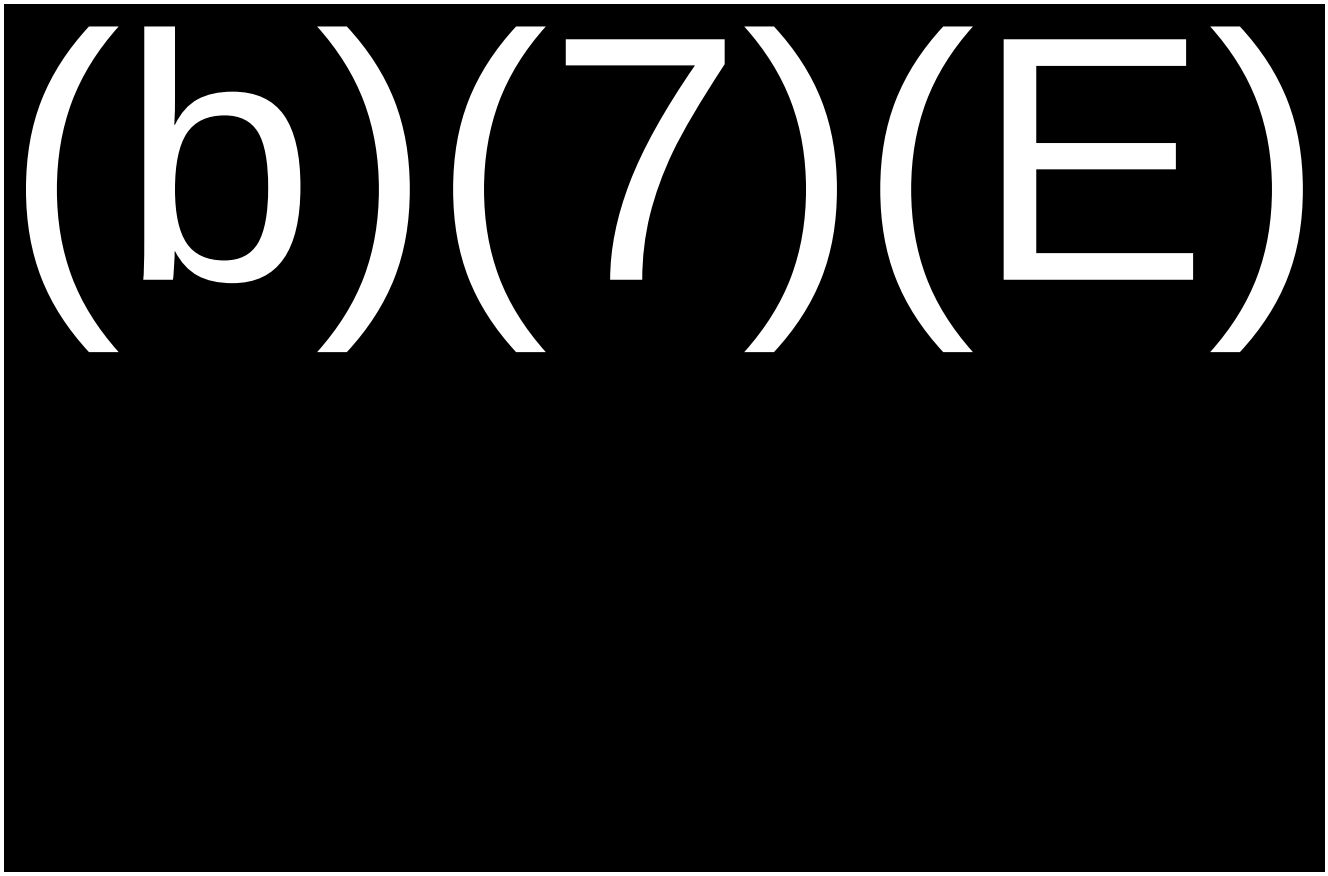


Figure 5. TravelerValidateRequest SOAP Message Example

4.4.2 Traveler End Request

The request to complete Traveler processing is initiated by the Kiosk System using the **TravelerEndRequest** message element. Submission of the **TravelerEndRequest** message is critical to the integrity of the APC Service. This message provides APC with confirmation of the final traveler information. Upon receipt, the APC Service initiates completion of traveler processing including manifest confirmation, when appropriate, and recording information the CBP Officer requires for traveler action. With the exception of a System Failure (SF) or Cancel (CA) referral prior to initiation of a dialogue with APC, no referral should be printed at the Kiosk until the corresponding **TravelerEndResponse** message is received. Receipt of a fault response in response to a TravelerEndRequest invalidates any prior referral assignment. When the kiosk cancels a session, any prior referral assignment is invalidated and the Traveler receipt should print a referral as specified by OFO in the Business Requirements.

Section 4.5.1specifies processing that the Kiosk must complete following receipt of the **TravelerValidateResponse** prior to formatting and transmitting the **TravelerEndResponse** message. As defined in this section, the kiosk must solicit flight confirmation for travelers eligible for confirmation processing.

APC waits up to 15 minutes from the time APC receives the **TravelerValidateRequest** message until the time APC receives **TravelerEndRequest** message for the traveler session. If the **TravelerEndRequest** message is not received within the 15-minute time window, the APC Service terminates the traveler session with no action; the traveler is locked out. If the APC

Service receives a **TravelerEndRequest** following the termination due to timeout, the APC Service will return a fault response specifying session not found. A timeout invalidates the original referral.

A **TravelerEndRequest** message should not be sent when the APC response to a kiosk request message is a fault. The fault message serves as notification to terminate any further processing of the traveler. If APC receives a **TravelerEndRequest** message following transmission of a fault message, APC will respond with another fault stating the "No traveler request found in cache." Reference Section 4.5.4 for information on fault handing.

In composing the **TravelerEndRequest** message, the **FlightManualIndicator** within the APIS Response Element should be set to false; this is a mandatory element.

The elements that comprise the **TravelerEndRequest** message are displayed in Table 14.

Table 14. TravelerEndRequest Element

TravelerEndRequest				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
KioskID	String	10	Y	A system wide unique identifier for the kiosk.
SessionID	String		Y	A value that uniquely identifies the session.
TravelerID	String		Y	The unique identification value associated with the traveler for the session
ApisResponse	ApisResponseType	--	M	Pre-arrival and departure manifest data either as provided by APIS. This is a mandatory element. The FlightManualEntryIndicator attribute should always be set='false'.
ReferralCodeResponse	String	2	N	The referral code assigned by the APC Service or a cancellation request for a traveler who is eligible for flight confirmation. Cancellation is only applicable to travelers who are eligible for flight confirmation. To cancel, the kiosk populates this field with TR. Except for cancel, return of a referral code different from that assigned by APC will generate a fault. Cancellation invalidates the original referral.

Table 15. ApisResponse Element

ApisResponse				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
AirlineCode	String	8	N	The code that identifies the airline of the flight or "AV" for Sea.
FlightNumber	String	20	N	The flight number or Vessel IMO number.
DepartureAirportCode	String	3	N	The IATA code of the port from which the flight/vessel departs
ArrivalAirportCode	String	3	N	The IATA code of the port in which the flight/vessel arrives. Note: The ArrivalAirportCode will sometimes be valued with the IATA code of the processing airport or an adjacent port code.
FlightManualEntryIndicator	Boolean	--	Y	**Always set to 'false'**.
DepartureCountryCode	CountryAlpha3Code	3	N	The code of the country from which the flight/vessel departs.
Address	AddressType		N	The address on the manifest

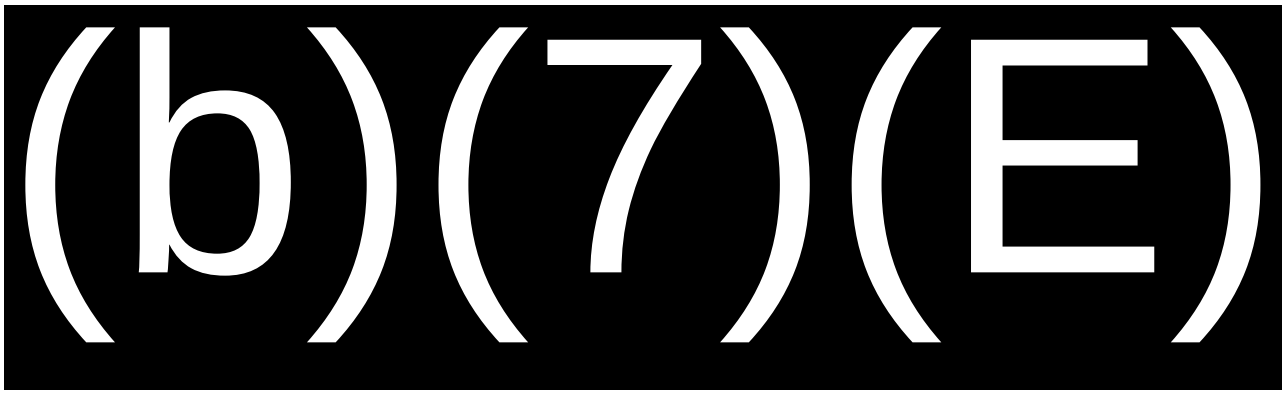


Figure 6. TravelerEndRequest SOAP Message Example

4.4.3 System Status Request

The request for the system status is initiated by the Kiosk System using the **SystemStatusRequest** message element. The **SystemStatusRequest** provides the kiosk vendor the status of the APC system and also enables APC to track the operational status of each APC site. For each site, each vendor must submit to APC one and only one **SystemStatusRequest** each minute that the site is operational. The restriction for only one **`SystemStatusRequest`** per minute per site/vendor is to ensure APC not be inundated with **`SystemStatusRequests.`** The elements that comprise the message request are displayed in

Table 16. Figure 7 shows an example of the **SystemStatusRequest** SOAP message.

Table 16. SystemStatusRequest Element

SystemStatusRequest				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
KioskID	String	10	Y	KioskID for the kiosk submitting the request. If other than a kiosk is submitting the request, a KioskID for the site should be provided

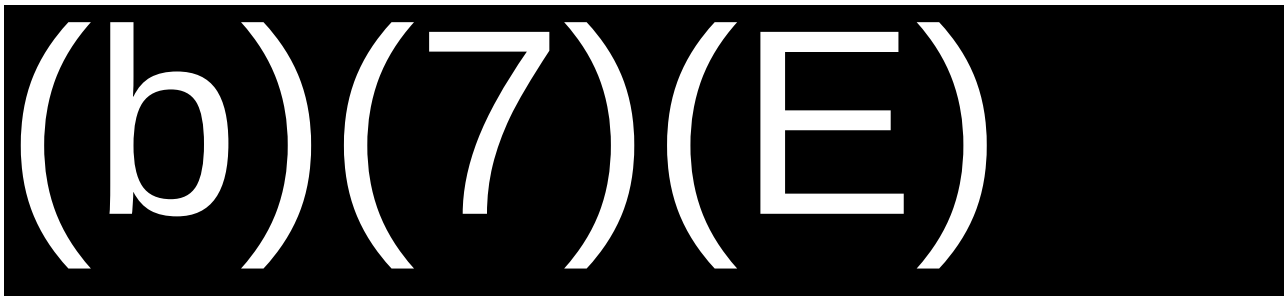


Figure 7. SystemStatusRequest SOAP Message Example

4.5 Response Messages

The APC Service will generate a response message to answer a request sent from the Kiosk System. Responses messages are:

- Traveler Validate Response
- Traveler End Response
- System Status Response
- Fault Element

In the following subsections, specifications are defined for each response message. Refer to Figure 2 for a depiction of the message dialogue between the Kiosk System and the APC Service. In addition, refer to Section 4.4 to review the corresponding request message specification.

4.5.1 Traveler Validate Response

The response to a **TravelerValidateRequest** is provided by the APC Service using the **TravelerValidateResponse** message element. The **TravelerValidateResponse** message acknowledges receipt of the **TravelerValidateRequest** message and provides to the kiosk a traveler referral code based on initial traveler vetting, subject to final processing. Receipt of the **TravelerValidateResponse** is not the basis for printing a receipt. The kiosk must receive the **TravelerEndResponse** prior to printing a receipt other than the SF or CA receipt.

When the referral code in the **TravelerValidateResponse** identifies a traveler eligible for flight confirmation, the Business Requirements require that stationary air kiosks request the traveler confirm his/her flight based on information the APIS Response element returned in the **TravelerValidateResponse** message.

Referral codes eligible for flight confirmation processing follow:

- PG (Passage Granted) (all Ports)
- DR (Declarations Referral) Applicable at ports authorized for enhanced declarations processing.

Consistent with the Business Rules, travelers who confirm the flight should be processed to normal completion. The kiosk should return the **TravelerEndRequest** with the referral code equal that provided in the **TravelerValidateRequest.**

Should a traveler fail to confirm presented flight information, the Kiosk should cancel the traveler session by returning a TR referral code in the **TravelerEndRequest**. Cancellation of the Traveler Session cancels the original referral code. The kiosk Vendor should refer to the OFO Business requirements for instructions on the referral to print for these travelers.

For travelers not eligible for flight confirmation (including all travelers processed at sea kiosks), the kiosk should send the **TravelerEndRequest** immediately upon receipt of the **TravelerValidateResponse**. The returned referral code should match the referral code in the **TravelerValidateResponse.**

If the kiosk attempts to cancel a passenger who is not eligible for flight confirmation, the APC Service will return a fault in the **TravelerEndRequest.** Additionally, except to cancel a traveler who is eligible for flight confirmation, the APC Service will return a fault in the **TravelerEndRequest** if the kiosk returns a **ReferralCodeResponse** that does not match the **ReferralCodeResponse** in the **TravelerValidateResponse**. As described above, the Kiosk notifies the APC Service to cancel a traveler by sending a TR Referral in the **TravelerEndRequest**. When the traveler is canceled, the original referral is invalidated.

The elements and child elements that comprise the message response are displayed in the tables that follow.

Table 17. TravelerValidateResponse Element

TravelerValidateResponse				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
KioskID	String	10	Y	The value submitted in the request message that uniquely identifies the servicing kiosk.
SessionID	String		Y	The value submitted in the request message that uniquely identifies the session.
TravelerID	String		Y	The value submitted in the request message that uniquely identifies the traveler for the session
ReferralCodeResponse	String	2	N	Preliminary referral code for the traveler. This is a 2 character string assigned by APC.
ApisResponse	ApisResponseType	--	Y	Pre-arrival and departure manifest data provided by APIS.
DailySecurityCode	String	15	N	A code generated daily to confirm

TravelerValidateResponse				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
				authenticity.

As discussed above, the **ApisResponseElement** is shared by the **TravelerEnd** Request Element and also by the Traveler Validate Response Element. When incorporated in the **TravelerValidateResponse** Element, the contents of this element reflect flight information for the traveler. When the traveler is found on a manifest, Carrier and flight data are populated. Flight and carrier data are null when a traveler is not found on a manifest. APC always sets **FlightManualEntryIndicator** to "false" in the **TravelerValidateResponse** Element.

Table 18. ApisResponse Element

ApisResponse				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
AirlineCode	String	8	C	The code that identifies the airline of the flight or "AV" for Sea. Populated when a traveler if found on a manifest; otherwise, null.
FlightNumber	String	20	C	The flight number or Vessel IMO number. Populated when a traveler if found on a manifest; otherwise, null.
DepartureAirportCode	String	3	C	The IATA code of the port from which the flight/vessel departs. Populated when a traveler if found on a manifest; otherwise, null.
ArrivalAirportCode	String	3	C	The IATA code of the port in which the flight/vessel arrives. Populated when a traveler if found on a manifest; otherwise, null. Note: The ArrivalAirportCode will sometimes be valued with the IATA code of the processing airport or an adjacent port code.
FlightManualEntryIndicator	Boolean	--	Y	Always populated "false".
DepartureCountryCode	CountryAlpha3Code	3	N	The code of the country from which the flight/vessel departs. Populated when a traveler if found on a manifest; otherwise, null.
Address	AddressType		N	The address on the manifest

Table 19. Address Element

Address				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
StreetNumberText	String	8	N	Street Number
StreetName	String	60	N	Street Name
AddressSecondary UnitText	String	35	N	Apartment or Unit Number
LocationCityName	String	70	N	City Name
LocationState	String	10	N	U.S. State Name
Location PostalCode	String	10	N	U.S. Postal Code

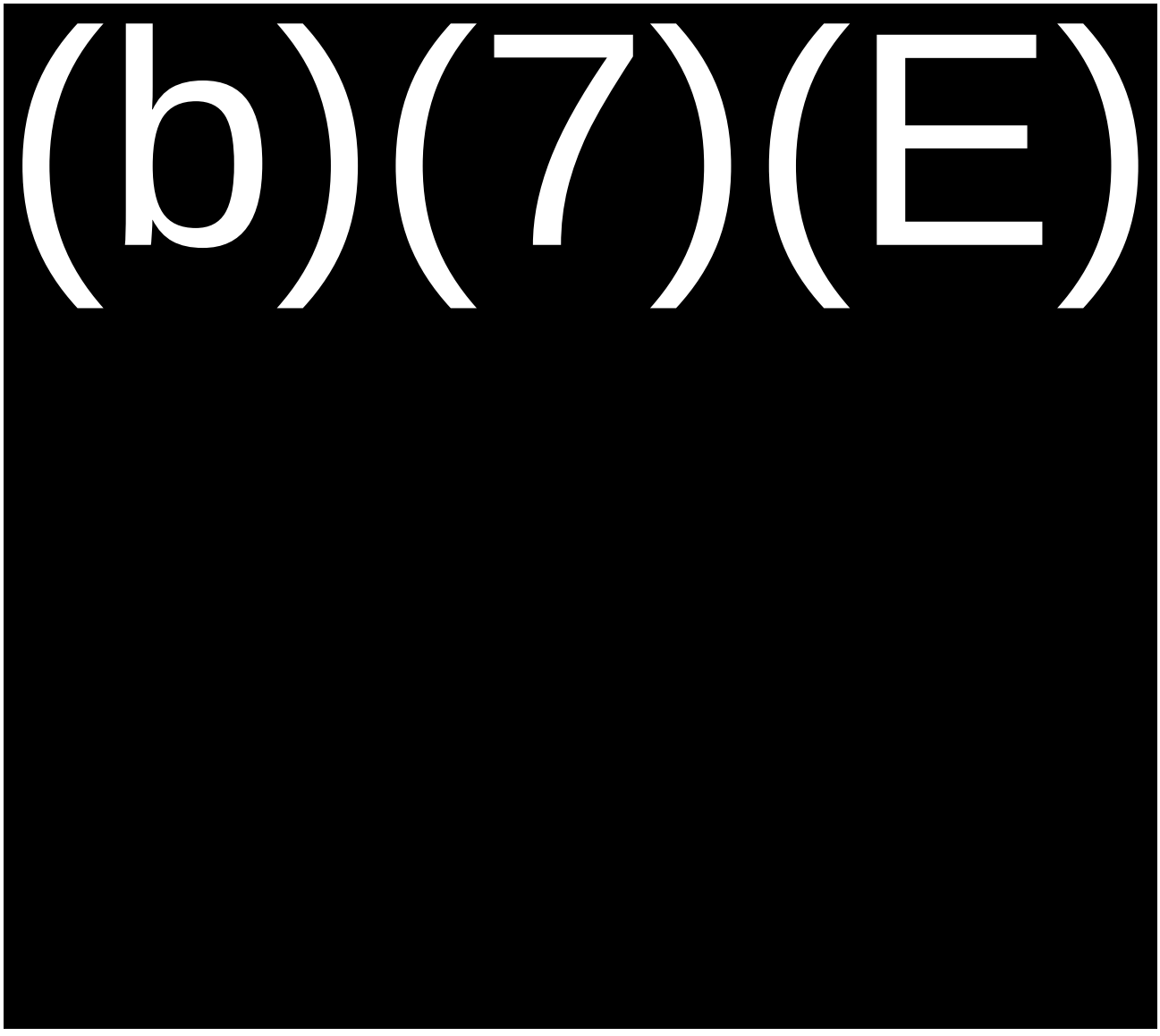


Figure 8. TravelerValidateResponse SOAP Message Example

4.5.2 Traveler End Response

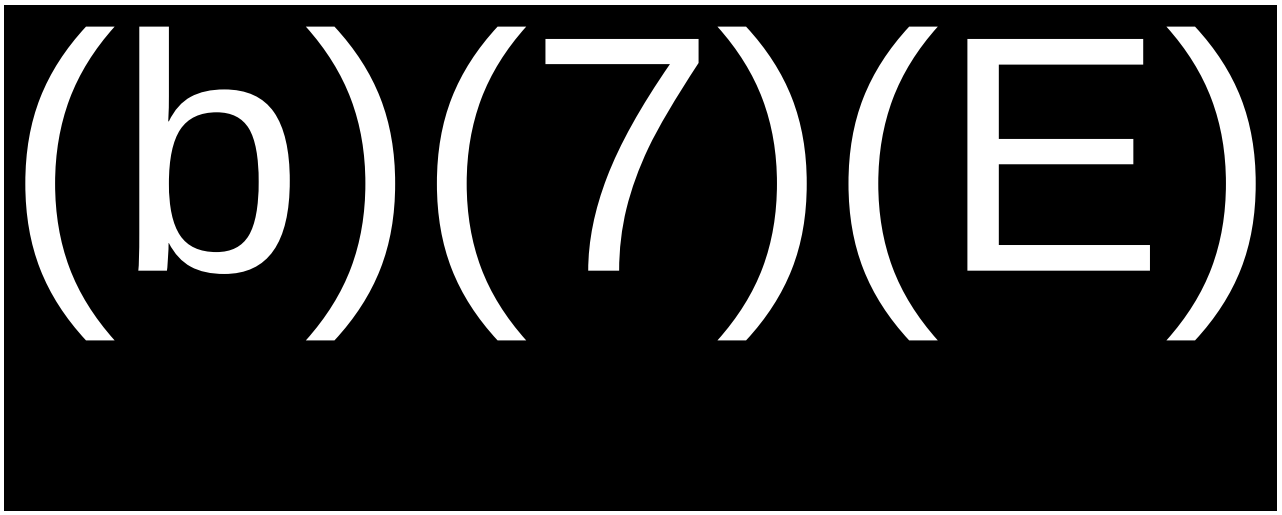
The **TravelerEndResponse** message is sent to the kiosk in response to the **TravelerEndRequest** as confirmation that all required processing for the traveler has been successfully completed. It is critical that the kiosk receive this response prior to printing any referral receipt. Receipt of a **TravelerEndResponse** authorizes the kiosk to complete processing of the traveler and print or display the referral receipt. Reference Section 5 for processing Referral Receipt codes.

If the APC server is unable to complete traveler processing normally, the APC server may return a fault response or the kiosk may timeout waiting for the APC response. Section 4.5.4 discusses kiosk response to receipt of a fault or a timeout condition.

The elements that comprise the **TravelerEndResponse** message are displayed in Table 20. Figure 9 shows an example SOAP message for the **TravelerEndResponse .**

Table 20. TravelerEndResponse Element

TravelerEndResponse				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
KioskID	String	10	Y	A system wide unique identifier for the kiosk.
SessionID	String		Y	A value that uniquely identifies the session.
TravelerID	String		Y	The unique identification value associated with the traveler for the session
AdmitUntilDate	Date	8	N	Admit Until Date; format conforms to NIEM standard



(b)(7)(E)

Figure 9. TravelerEndResponse SOAP Message Example

4.5.3 System Status Response

The response for system status is provided by the APC Service using the **SystemStatusResponse** message element. The elements and child elements that comprise the message response are displayed in Table 21. Figure 10 shows an example **SystemStatusResponse** SOAP message.

Table 21. SystemStatusResponse Element

SystemStatusResponse				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
KioskId	String	10	Y	KioskID for the requesting site.
SystemStatusIndicator	Boolean	--	Y	The APC Service status indicator. A true value indicates that the system is up; a value of false indicates that the system is down.

(b)(7)(E)

Figure 10. SystemStatusResponse SOAP Message Example

4.5.4 Fault Response

The APC Service returns a fault response (<soap:Fault>) in response to processing errors which may occur during traveler processing. A fault response may be returned following APC receipt of either a **TravelerValidiateRequest** or a **TravelerEndRequest** message. The fault response terminates processing for the traveler. A fault response to a **TravelerEndRequest** message invalidates any initial referral.

When a fault is returned, the APC service will not return the normal dialogue message; i.e., the **TravelerValidateResponse** will not be returned when the fault occurs during traveler validate processing and the **TravelerEndResponse** message will not be returned during traveler end processing.

A fault may be returned for numerous reasons, examples of which are identified in Table 25. The specific reason for each fault is embedded in the fault message. The elements that comprise the Fault message are defined in Table 22. Figure 11 shows an example SOAP message for a fault response. Return of a fault signals termination of traveler processing.

Following receipt of a fault response, the Kiosk should not send any further requests to APC for the traveler. When APC sends the Fault message in response to a **TravelerValidiateRequest** message, the kiosk should not send the **TravelerEndRequest** message. If APC receives a **TravelerEndRequest** message following transmission of a fault message, APC will respond with another Fault message. This subsequent fault message will normally state "No traveler request found in cache."

Although the fault response terminates all processing for the individual traveler session, when the session is a multi-party session, processing of other travelers within the session should continue normally. The fault response applies only to the specific traveler within the session.

Table 22. Fault Element

Fault Element				
Attribute	**Data Type**	**Size**	**Rqd**	**Description**
KioskID	String	10	N	A system wide unique identifier for the kiosk.
SessionID	String		N	The unique session identifier.
TravelerID	String		N	The unique identification value associated with the traveler for the session
FaultCode	String	10	Y	The fault code associated with the error condition identified by the system.
FaultCodeDescription	String	40	Y	A description of the fault.

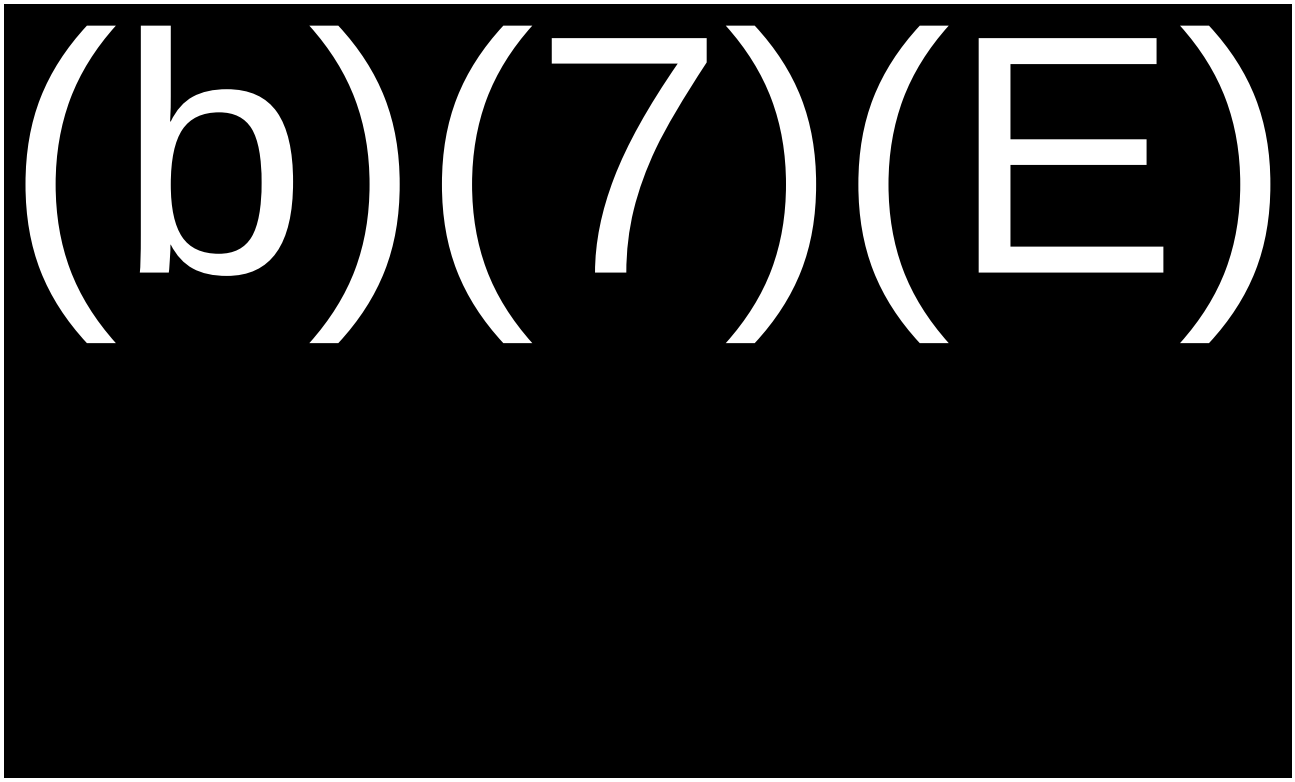


Figure 11. SOAP Fault Message Example

5. Receipt Referral Codes

APC has employs a two character Referral Code. Referral codes generated by APC are not restricted to a defined subset; Kiosks are authorized to assign referral codes CA and SF.

With the exception of the System Failure (SF) and Cancel (CA) referral codes and some instances of the AP referral, kiosks must print on the Referral Receipt the exact referral received from the APC Service; when the Kiosk receives a fault response from APC, the fault invalidates the preliminary referral and the Kiosk should print a SF (System Failure) Receipt.

The kiosk vendor should refer to OFO and the Business requirements on how to handle the following instances:

- The traveler or kiosk discontinued processing prior to transmission of the Traveler Validate Request message.
- A traveler eligible for flight confirmation elected to cancel confirmation following receipt of a valid referral code in the **TravelerValidateResponse** message.

The APC schema does not include an enumeration element for Referral Codes. This element has been defined as a simple type; the Kiosk should accept whatever code is sent by APC. This provides flexibility to expand and/or change specific codes in the future.

Table 23. Kiosk Generated Referral Codes

Referral Condition	Referral Code	Referral Description
Cancel	CA	Designates cancellation of the traveler session. This referral code is printed by the Kiosk for each traveler whose session is cancelled by the Kiosk for those instances where specific OFO guidance is not specified in the Business Requirements.
System Failure	SF	Designates termination of traveler processing due to a system error. This referral is local to the Kiosk system. As such it will not be sent by the APC service nor should it be returned to the APC service.

6. Communications

6.1 IP Addresses

Each site must provide CBP a publically routable IP address to be used in the Production environment and a separate IP address to be used in the Non-Production environment. If failover is included in the network design, IP addresses for each server should be provided. CBP recommends that a site provide no more than four (4) IP addresses to CBP. Receipt of the IP addresses is prerequisite to initiating a request to CBP to open the firewall.

The IP addresses must be sent to APC OIT GROUP(b) (7)(E) in an encrypted file; the encryption password ***must*** be sent in separate correspondence. Failure to follow these procedures will render the submitted IP addresses obsolete; new IP addresses will be required. Note: Word documents may be password protected; emails transmitting the document should be encrypted. Alternatively, the IP addresses can be pasted in an email that is encrypted for transmission.

Firewall requests are implemented based on Priority set by the Program Office (OFO); these priorities reflect the priority across all of DHS. Prior to (or concurrent with) submission of the IP addresses to OIT, the vendor is responsible for securing OFO's approval for OIT to act on the request. Once OIT has received the OFO approved IP request, OIT will submit a request to the responsible parties within CPB to open the firewall. The APC System Onboarding guide specifies document lead times applicable to these requests.

6.2 2-way SSL Certificates

The communication between the Kiosk System and the APC Server occurs via a two-way SSL connection utilizing mutual authentication.

Certificates need to be either VeriSign or Entrust. Both of these are certified in the Federal Information Processing Standards (FIPS), a standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology (NIST).

Each port will utilize a single SSL Certificate to communicate with the CBP production site. A separate SSL certificate will be required for communication between the port non-production environment and CBP's non-production (test) environment. The one non-production certificate will be used for communication with both the CBP System Acceptance Test (SAT) and the CBP Quality Assurance (QAX) environments.

Prior to establishing communication between the systems, the APC Service will need to register the Kiosk System's:

- publicly routable IP address
- public certificate (2048 bits) from a CBP approved Certificate

In addition, the Kiosk System will need the APC Service's Certificate Authority certificate chain to authenticate the APC Service.

To successfully connect to the APC Service both parties must exchange and install the certificates prior to initiating the SSL conversation. Figure 12 illustrates the certificate configuration for two-way SSL authentication between two applications.

The certificates must be sent to the APC OIT GROUP (b) (7)(E) s encrypted files; the encryption password(s) must be sent in separate correspondence. Failure to follow these procedures will render the submitted certificates obsolete; new certificates will be required.

Note: Word documents may be password protected; emails transmitting the document should be encrypted.

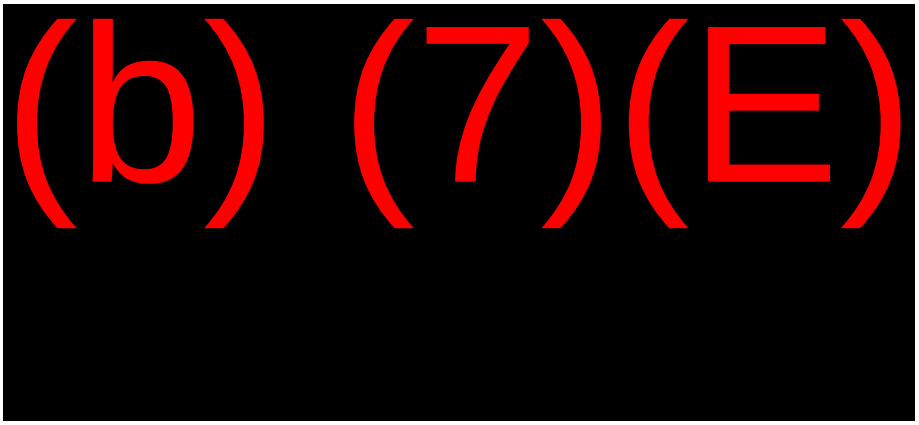


Figure 12. Two-Way SSL Authentication

The SSL client (the APC Kiosk Server) initiates a connection to the SSL server (the APC

Service) by opening a connection to the SSL server. Next, the SSL server presents its certificate to the SSL client for verification and then requests that the SSL client present its certificate to the SSL server for verification. Once this protocol is completed and the certificates match then the communications dialogue between the Kiosk System and the APC Service may commence.

7. Security and Integrity

The Kiosk System is hosted on a port's network. The interface protocol between the port network and the APC Service will be HTTPS/SOAP XML messages sent to and from an XML appliance and the Kiosk System. The XML appliance provides an isolation layer that protects the security and integrity of the CBP network. The SSL certificates and IP addresses, port number information, protocols, virus software and other technical controls are configured to ensure the security and information integrity of the CBP network. AES-256 encryption is required for messages sent from the kiosk to CBP.

Message information integrity is maintained through the use of XML and XSD validation schemas to ensure that each transaction is unique and accurate.

The Kiosk System shall not store any privacy sensitive data such as MRZ data, personal traveler data or referral codes.

7.1 (b) (7)(E)

(b) (7)(E)

7.2 Malware Protection

In Accordance with DHS System Security Policy Directive 4300A Section 5.6 Malware Protection: There are a number of programs that are classified as malicious code, or "malware." These programs are referred to as viruses, logic bombs, worms, Trojan horses, and other names. This section covers types of malware.

7.2.1 Types of Malware

Various types of malware are defined below:

Virus – A virus is a self-replicating malicious program segment that attaches itself to legitimate application programs, operating system commands, or other executable system elements and

spreads from one system to another. Another definition for virus is: a program or piece of code that is loaded onto a computer without the user's knowledge and runs against the user's wishes. As it spreads, it is said to be *infecting* the system

Worms – Worms are malicious programs that copy themselves from system to system, rather than infiltrating legitimate files. For example, a mass-mailing email worm is a worm that sends copies of itself via email. A network worm makes copies of itself throughout a network or through file shares. Worms often contain Trojan horse or "backdoor" programs.

Logic Bombs – A logic bomb can be defined as dormant code, the activation of which is triggered by a predetermined time or event. For example, a logic bomb might start erasing data files when the system clock reaches a certain date or when an application has been loaded X number of times.

Trojan Horses – A Trojan horse is a computer program that is apparently or actually useful but performs another function covertly. A Trojan horse generally provides remote access to an unauthorized person. A Trojan horse can be used to modify databases, write checks, send email, or destroy files. It could be imbedded by a programmer or downloaded from the Internet.

Web Bugs – A web bug is executable code included in an image (as small as one pixel) that can disrupt the operation of a system or acquire and transmit information from a system without the s knowledge of users who merely visit a malicious or compromised (bugged) web site.

Backdoor – A backdoor is a method of bypassing a system's security controls. The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.

7.2.2 How Malware Affects Systems

Malware poses a significant threat to DHS systems therefore, *it is essential that all systems employ preventive measures commensurate with the level of risk identified in the risk analysis.* What makes malware unique is that it can spread from program to program and from system to system *without direct human intervention*.

Systems that can be accessed by DHS-approved browser configurations should be categorized (trusted, untrusted, etc.). Users shall not deploy Web browsers "out of the box," since the security policies implemented in such tools tend to reflect vendor interests that do not coincide with DHS interests.

7.2.3 Procedures when Malware Is Detected on the Systems

If malware is detected, the LAN/system administrator is responsible for taking appropriate actions, including:

- Running disinfectors available with antivirus software.
- Scanning backups for malware prior to restoring system applications and data files.
- Checking for re-infection from media overlooked during the eradication process.

- Using incident reporting procedures notify the CBP ISSO of the security incident by sending an e-mail to the (b) (7)(E) (b) (7)(E)
- Once the malicious code has been eradicated, the system administrator shall determine the extent of the damage and restore the cleaned programs and files to the disinfected system.

Occurrence of malicious code constitutes a *security incident* that must be reported to the CBP ISSO.

7.2.4 Strategies to Prevent Malware

To prevent Malware security incidents the port authority or port authority contractor shall implement a defense-in-depth strategy that:

1) Installs antivirus software on kiosks and servers.
2) Configures antivirus software on kiosks and servers to check all files, downloads, and email.
3) Installs updates to antivirus software and signature files on kiosks and servers in a timely and expedition's manner without requiring the end user to specifically request the update. (Minimum Monthly).
4) Installs security patches to kiosks and servers in a timely and expeditious manner (Monthly).
5) Servers and Kiosk Operating systems shall be scanned monthly utilizing credentialed Tenable security center with results being sent to the CBP ISSO on a monthly basis in both PDF and .nessus format. In accordance with (DHS System Security Policy Directive 4300A Section 4.9 Department Information Security Operations).

8. Environment Information

The APC Service maintains both Test and Production environments. Connection to CBP APC Service should be configured with the Fully Qualified Domain Names and not the External IP Addresses. IP Addresses are subject to change in the event of server conversions.

(b) (7)(E)

- Environment
- Fully Qualified Domain Name (FQDN)
- External IP Addresses
- External Port
- Specification of requirement for Certificate Setup (required for all environments)
- URL of the end point for the service to call the methods

URL of the end point for the service to request the WSDL

9. Processing Time Specifications

Table 24 describes the following information:

- Average Transaction Load per day per kiosk (TPD) – This value indicates, on average, the number of request/response transaction pairs that are being processed per day per kiosk.
- Expected Average Response Time per Transaction – The expected average time, in seconds, APC Service will take to process the entire request and response transaction.
- Timeout per Transaction – The time, in seconds, after which APC Service will timeout if the transaction has not completed processing.

All values are calculated based on current production information evaluated during November 2013. As more travelers are processed via APC as a result of additional kiosk stations in existing and new locations then the TPD values may increase. Fluctuations in the transaction volume may affect transaction processing times. Thus, an increase in the transaction load may cause an increase in the response time.

Table 24. APC Service Message Time Specification

Message Name	Average Transaction Load per day per kiosk (TPD)	Expected Average Response Time per Transaction (seconds)	Timeout per Transaction (seconds)
Traveler Validate Request / Response	15000	10	30
Traveler End Request / Response	15000	10	30

10. Special Processing

There are no special processing requirements.

11. Sample Fault Messages

Table 25 below provides a sample of fault messages that may be generated by the APC Service. This is not an inclusive list of fault message. A fault message terminates Traveler processing regardless of where in the processing sequence the fault occurred. A referral receipt should not be printed for any traveler whose processing terminates with a fault.

Table 25. Sample APC Service Fault Messages

#	Soap: Reason
1	(b)(7)(E)
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	

#	Soap: Reason
26	(b)(7)(E)
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	

12. Open Item Discussions

This section will contain items and information that needs to be clarified through this document and other items that needs to be discussed between the two parties involved with this exchange. Please see Table 26 for a list of Open Discussion items.

Table 26. APC Service Open Discussion Items

Item #	Title	Description

Appendix A Facial Image Capture

APC FACIAL IMAGE CAPTURE SPECIFICATION STANDARDS & BEST PRACTICES

Best practices for capturing facial photos that could be used for facial recognition focus primarily on image quality.

MAXIMIZING FACIAL IMAGE QUALITY

The quality of facial images dramatically impacts the performance of all facial recognition algorithms. NIST has shown that the accuracy (true accept rate) is orders of magnitude worse for poor quality web cam photos from unstructured environments compared to images captured in well controlled environment such as Passport photos.

Facial images captured at the kiosk shall conform to International Civil Aviation Organization (ICAO) standards (ISO 19794-5). In addition, the following standard shall also be followed: ANSI/NIST-ITL 1-2011: Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information. The following sections should be referenced:

- 7.7.5 Subject acquisition profile/SAP/FAP/IAP
- Annex E: Facial Capture Requirements and Recommendations

In general, it is highly recommended that multiple facial images be automatically captured using a "quality in the loop" approach that continuously measures image quality parameters and makes automated adjustments such as lighting, focus, etc. In addition, it is recommended that the facial 1:1 verification match score also be used as a part of the quality loop.

Specific quality parameters that describe features of facial images and recommended best practices for optimizing the parameters are described in the next sections.

Image Resolution, Size and Color

A very low resolution live photo captured at the kiosk will result in decreased match performance. However, there is little benefit in very high resolution photos. Facial images shall be at least 480 pixels in width and 640 pixels in height with an optimal resolution of 768 pixels by 1024 pixels. In terms of resolution:

- Optimal - greater than or equal to 0.75 megapixels
- Satisfactory - greater than or equal to 0.30 megapixels but less than 0.75 megapixels
- Unacceptable - less than 0.30 megapixels

The face shall be centered in the overall image and be greater than 50% of the frame width and greater than 75% of the frame height with greater than 90 pixels from pupil to pupil. Images shall be captured in 24 bit color. Images shall possess true symmetry and not be reversed mirror images.

Lighting

Proper lighting is one of the more difficult requirements for photo capture due to the wide variations in the temporal and spatial characteristics of natural and synthetic lighting conditions across the airport environment. It is highly recommended that the kiosk have multiple self-contained adjustable lighting sources that automatically adjust left, right, top and bottom illumination levels to ensure a uniform light intensity across the traveler's face. Specific illumination requirements include:

- Illumination shall at a minimum be 3-point source to minimize shadows and eliminate hot spots on the face
- Light sources shall employ diffusers
- Sufficient lighting shall be installed such that luminance on the properly positioned face exceeds 500 lux
- The region of the face from the crown to the base of the chin and from ear to ear shall be clearly visible and free of shadows, particularly, there shall be no dark shadows in the eye-pockets due to the brow
- The iris and pupil of the eyes shall be clearly visible
- Lighting shall not create shadows in the background
- Lighting shall create natural looking skin tones
- "Red-eye" is not acceptable

Pose

The pose of the head has a significant impact to facial match algorithm performance. Since most facial recognition applications will compare the APC live photo to a standard ICAO passport photo pose, it will be important that the live photo not deviate from the ICAO standards.

- The pose will consist of the full-face or frontal pose
- The body shall be rotated in alignment with the head
- The yaw, pitch and roll rotations for the head shall not exceed 5 degrees
- Utilize automatic camera height adjustment to ensure that a full frontal image can be captured without the traveler bending their neck
- The eyes shall be open
- The expression shall be neutral with the mouth closed

Composition

Image composition is another parameter that is difficult to control in the unstructured and dynamic airport environment. The following requirements should be optimized as much as possible.

- The image background should be as neutral as possible. Avoid bright lights such as overhead sources or bright windows
- Utilize operational controls to prevent other faces such as family members from being in field of view

- Head coverings such as hats or scarves should not be worn. The full face and ears must be entirely visible
- Travelers should be instructed to move long hair away from face
- For travelers that normally wear eye glasses, the glasses should not be removed
- Dark or heavily tinted glasses should not be worn
- Lighting should be adjusted so as not to reflect from the glasses
- In general, traveler instructions such as wearing glasses should be used to optimize the similarity between the composition of the live photo and the passport photo

Traveler height

Tall and short individuals should be accommodated by the APC kiosk.

- The camera should collect photographs of subjects up to 6’5’’ so that the crown of the head is visible
- The camera should collect photographs of subjects down to 5’5’’ so that their neck below the chin is visible.
- It is recommended that individuals whose height is not within the range 5’5’’ to 6’5’’ should be detected e.g. by face finding failure, and referred to traditional primary inspection.

Camera lens and mounting should be selected to maximize the distance to the traveler to ameliorate fish-eye effects. The subject should stand at arm’s length. This can be achieved by having a tray at or below waist height.

Appendix B Abbreviations

Abbreviation	Definition
APC	Automated Passport Control
APIS	Advance Passenger Information System
ATDS	Airport Technical Design Standard
CBP	U.S. Customs and Border Protection
CBSA	Canadian Border Services Agency
FIS	Federal Inspection Services
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
IEPD	Information Exchange Package
NDC	National Data Center
NIEM	National Information Exchange Model
PII	Personally identifiable information
SSL	Secure Sockets Layer
WSDL	Web Services Definition Language